

2:23-mj-01166 DBP

**AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEIZURE WARRANT**

I, Juan Muñoz, a Special Agent (“SA”) with Homeland Security Investigations (“HSI”),
being duly sworn, declare and state as follows:

PURPOSE OF THE AFFIDAVIT

1. I am submitting this affidavit in support of an application for warrant to seize virtual currency, also known as “cryptocurrency,” which was stolen from at least three identified victims.

2. The United States seeks seizure of all cryptocurrency including all Bitcoin (“BTC”), Ethereum (“ETH”), Tether (“USDT”), and Cardano (“ADA”) from cryptocurrency wallet address **3HS1CV9nYZQs3D5Nm7PLZSWwshJxu6xyWE** (“xyWE”) held by OKX in account **305340717360944980** belonging to **Su Chaoling** (“SUBJECT ACCOUNT”).

3. For the reasons described below, there is probable cause to believe the SUBJECT ACCOUNT is subject to seizure and forfeiture as follows:

Criminal Seizure and Forfeiture:

- a. Pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c) because the SUBJECT ACCOUNT is derived from proceeds traceable to a violation of 18 U.S.C. § 1343 (Wire Fraud). Section 981(a)(1)(C) provides for the civil forfeiture of any property, real or personal, which constitutes or is derived from proceeds from any offense constituting a “specified unlawful activity” as defined in 18 U.S.C. § 1956(c)(7), or a conspiracy to commit such offenses. A “specified unlawful activity,” as defined in § 1956(c)(7), includes offenses listed in 18 U.S.C. § 1961(1). Section 1961(1) includes violations of 18 U.S.C. § 1343. Section 2461(c) provides for forfeiture authority in criminal

cases where civil forfeiture is authorized.

- b. Pursuant to 18 U.S.C. § 982(a)(1) because the SUBJECT ACCOUNT was involved in a violation of 18 U.S.C. § 1956 (money laundering), or was traceable to such property.
- c. Consequently, seizure of the SUBJECT ACCOUNT for criminal forfeiture is authorized by 21 U.S.C. § 853(f) and 18 U.S.C. § 982(b).

Civil seizure and forfeiture:

- a. Pursuant to 18 U.S.C. § 981(a)(1)(C) because the SUBJECT ACCOUNT is property, real or personal, that constitute or is derived from proceeds traceable to violations of 18 U.S.C. § 1343 (Wire Fraud) or conspiracy to commit the same.
- b. Pursuant to 18 U.S.C. § 981(a)(1)(A) because the SUBJECT ACCOUNT was involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956, or is traceable to such property.
- c. Consequently, seizure of the SUBJECT ACCOUNT for civil forfeiture is authorized by 18 U.S.C. § 981(b).

4. 18 U.S.C. § 1343 states:

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio or television communication in interstate or foreign commerce, any writings, signs, signals, pictures . . . for the purpose of executing such scheme or artifice.

5. 18 U.S.C. § 1956 states in relevant part:

Whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity—

(B) knowing that the transaction is designed in whole or in part—

(i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity.

6. A restraining order for the assets under 21 U.S.C. § 853(e) would likely not be sufficient to adequately protect the assets and so a seizure warrant pursuant to 21 U.S.C. § 853(f) is necessary. Cryptocurrency is easily removed or transferred from a wallet and only seizure assures that the crypto currency will be available for forfeiture. I am also aware that courts have held that criminal seizure, instead of restraint, is appropriate when assets are fungible and readily transferable. *See, e.g., United States v. Dupree*, 781 F. Supp. 2d 115,133 (E.D.N.Y. 2011) (citing *United States v. Daccarett*, 6 F.3d 37, 49 (2d Cir. 1993) (holding that “seizure under the criminal statutes was thus appropriate because the seized funds could be, and had been, easily transferred in and out of the accounts)); *see also United States v. Martin*, 460 F. Supp. 2d 669, 677 (D. Md. 2006) (“Given the fungible and readily transferable nature of the property . . . and the size and seriousness of this alleged conspiracy . . . this Court cannot conclude that there was no probable cause to believe that a seizure warrant was necessary to secure the property”).

AFFIANT BACKGROUND & INVESTIGATION INVOLVEMENT

7. As a SA with HSI since September 2015, I am currently assigned to the HSI Salt Lake City Office where my duties are to conduct investigations related to financial crimes and cybercrimes. During my career as an HSI SA, I have participated in numerous financial crime related investigations. I have received both formal and informal training from HSI and other institutions regarding financial and cyber related investigations. Prior to working as an HSI SA, I was a Border Patrol Agent with the United States Border Patrol from 2008 to 2015.

8. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and

witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not purport to set forth all my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only. Unless specifically indicated otherwise, all dates set forth below are “on or about” the dates indicated, and all amounts or sums are approximate.

STATEMENT OF PROBABLE CAUSE

A. Training and Experience Regarding Cryptocurrency

9. From my training and experience investigating cryptocurrency transactions and crimes involving the use of cryptocurrencies, I know the following:

- a. “Cryptocurrencies” or “virtual currencies” are digital asset designed to work as a medium of exchange that uses cryptography to secure financial transactions, control the creation of additional units of the currency, and verify and transfer assets. BTC, ETH, USDT, and ADA are popular types of the many cryptocurrencies available.
- b. Transactions involving cryptocurrency are often recorded and visible on a public ledger called a blockchain, where each transaction is referred to by a lengthy series of letters or numbers that identify the “address” from which the funds were transferred, and the destination to which the funds were sent. Each type of cryptocurrency has its own blockchain that reflects all transactions in that currency. Analysis of the blockchain can essentially allow the public to see and track cryptocurrency transactions.
- c. Cryptocurrency stored at a particular address is typically accessed using secret or

private encryption “keys,” which are commonly stored using a software “wallet”.

Those keys are essentially the password needed to access the cryptocurrency stored at a particular address. Only the holder of the key can access or transfer cryptocurrency out of an address.

- d. Cryptocurrency “exchanges” are clearinghouses that allow for exchange between different types of cryptocurrencies, or between cryptocurrency and fiat currency (e.g., United States dollars). Some exchanges also allow users to create accounts and store cryptocurrency with the exchange, like a bank account. In those instances, the cryptocurrency is often stored in an address or series of addresses owned and controlled by the exchange operator. Cryptocurrency exchanges operate both inside and outside of the United States.
- e. Virtual asset service provider (“VASP”): A VASP is a business that conducts one or more of the following activities or operations for or on behalf of another natural or legal person:
 - i. exchange virtual currencies for fiat currencies (currencies established by government regulation or law), and vice versa;
 - ii. exchange virtual currencies for one or more forms of other virtual currencies;
 - iii. transfer virtual currencies;
 - iv. safekeep and/or administer virtual currencies or instruments enabling control over virtual currencies; and participate in and provide financial services related to an issuer’s offer and/or sale of a virtual currency.

Many VASPs collect Know Your Customer (“KYC”) information, such as names,

e-mail addresses, and IP addresses, regarding their users.

- f. The cryptocurrency transactions discussed in this affidavit involves BTC, ETH, USDT, and ADA. These currencies are traded and sold by many exchanges.
- g. BTC is a cryptocurrency allegedly created by Satoshi Nakamoto. As of December 6, 2023, 1 BTC was worth approximately \$43,956.94 United States Dollar (“USD”).
- h. ETH is a cryptocurrency allegedly created by Vitalik Buterin. As of December 6, 2023, 1 ETH was worth approximately \$2,261.40 USD.
- i. USDT is a cryptocurrency stablecoin, launched by the company Tether Limited Inc. As of December 6, 2023, 1 USDT was worth approximately \$1.03 USD.
- j. ADA is a cryptocurrency allegedly created by Charles Hoskinson. As of December 6, 2023, 1 ADA was worth approximately \$.43 USD.

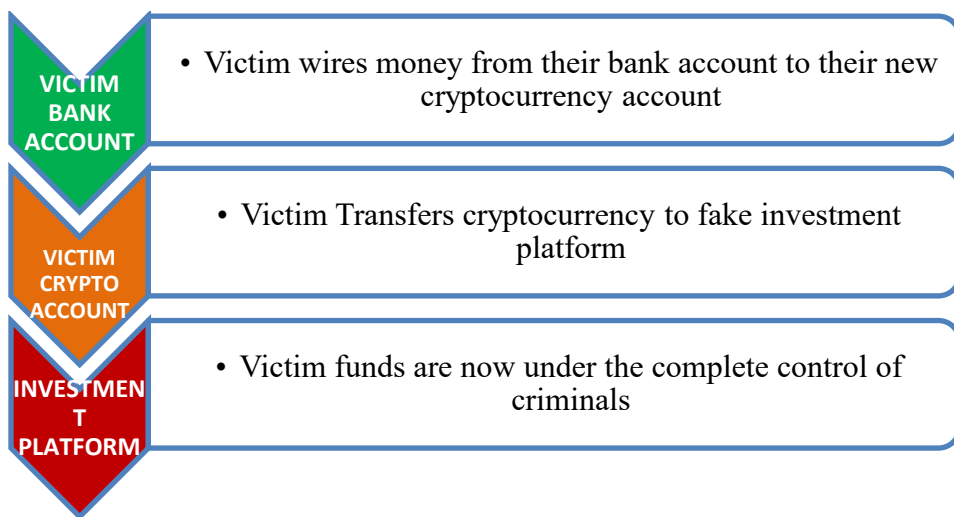
B. Background of Investigation

PIG BUTCHERING DEFINED

9. HSI and United States Secret Service (“USSS”) are investigating an investment fraud scheme, referred to as “pig butchering,” a term derived from the foreign-language word used to describe this scheme. Based on data submitted to the FBI’s Internet Crime Complaint Center (located at <https://www.ic3.gov/>), in 2022 alone, pig butchering schemes targeted tens of thousands of victims in the United States and resulted in over two billion dollars in private assets being siphoned overseas. Pig butchering schemes begin by criminals contacting potential victims through seemingly misdirected text messages, dating applications, or professional meetup groups. Next, using various means of manipulation, the criminal gains the victim’s affection and

trust. Criminals refer to victims as “pigs” at this stage because they concoct elaborate stories to “fatten up” their victims.

10. Once that trust is established, the criminal recommends cryptocurrency investment by touting their own, or an associate’s, success in the field. Means of carrying out the scheme vary, but a common tactic is to direct a victim to a fake investment platform hosted on a website. These websites, and the investment platforms hosted there, are created by criminals to mimic legitimate platforms. The subject assists the victim with opening a cryptocurrency account, often on a U.S.-based exchange such as Coinbase, and then walks the victim through transferring money from a bank account to that cryptocurrency account. Next, the victim will receive instructions on how to transfer their cryptocurrency assets to the fake investment platform. On its surface, the platform shows lucrative returns, encouraging further investment; underneath, all deposited funds are routed to a cryptocurrency wallet address controlled completely by the criminals – the “butchering” phase of the scheme.



11. Pig butchering perpetrators frequently allow victims to withdraw some of their “profits” early in the scheme to engender trust and help convince victims of the legitimacy of the platform. As the scheme continues, victims are unable to withdraw their funds and are provided

various excuses as to why. For example, the criminals will often levy a fake “tax” requirement, stating taxes must be paid on the proceeds generated from the platform. This is just an eleventh-hour effort by the criminals to elicit more money from victims. Ultimately, victims are locked out of their accounts and lose all their funds.

12. On October 24, 2023, I was notified by West Valley City Police Department regarding a local Utah-based victim (“Victim 1”) who was defrauded out of approximately 1.63659 BTC through a pig butchering scheme. Through forensic analysis, investigators were able to trace six separate transactions the victim made to the SUBJECT ACCOUNT.

13. OKX provided an account number for the SUBJECT ACCOUNT wallet and identification of the account holder. As an exchange, OKX follows KYC rules and obtains identifiable information on all their customers. OKX provided account number 305340717360944980 opened on 4/27/2022 and identified the account owner as Su Chaoling, a Philippine national. As of November 9, 2023, the account contained approximately \$287,046.91 USD worth of cryptocurrency. OKX agreed to freeze the account for 14 days to allow law enforcement to obtain a seizure warrant for the stolen BTC funds.

14. On November 13, 2023, as a result of the initial investigation involving Victim 1, Magistrate Judge Daphne A. Oberg granted the government’s application for a seizure warrant authorizing the seizure of up to 1.63659 BTC (At the time, 1.63659 BTC was worth approximately \$58,160.54 USD) to be seized from the SUBJECT ACCOUNT (Case No. 2:23mj1061-DAO).

15. On November 29, 2023, I was informed by OKX that another law enforcement agency was also investigating the SUBJECT ACCOUNT. OKX provided contact information for United States Secret Service Special Agent Alen Krso. I spoke with SA Krso and he provided me

with information of additional victims whose funds were also traced to the SUBJECT ACCOUNT to include a recent seizure by Jupiter Police Department in the State of Florida where the victim's (Victim 2) funds were traced to the SUBJECT ACCOUNT.

16. On September 11, 2023, Jupiter Police Department Detective L. Jurac obtained a State of Florida seizure warrant to seize up to .3224163 BTC which was traced to the SUBJECT ACCOUNT as a result of a pig butchering scheme involving a victim in the state of Florida. A total of six (6) transactions were traced but only four (4) of the 6 transactions were traced to the SUBJECT ACCOUNT (Jupiter Police Department Case# 23003294).

17. On September 20, 2023, OKX complied with the State of Florida seizure warrant and transferred .32224 BTC to Jupiter Police Department's Coin Base Wallet address.

18. I reviewed the trace analysis from Jupiter Police Department and noticed that after the initial deposit of Victim 1 and Victim 2's money, their money was moved to the same intermediate wallet, **3BdhHWqcM4wox8ESLVkWxrVLHn647EE6oy** ("E6oy"), before the ultimate transfer of their money to wallet **xyWE** in the SUBJECT ACCOUNT. The transactions were done on different days and times and I know from my training and experience that perpetrators involved in these types of schemes will utilize the same wallet addresses to receive funds from different victims to facilitate the movements of the fraudulent transactions.

19. On November 29, 2023, SA Krso informed me of at least 6 victims who deposited money into an investment site called curve.bet and all of whom were unable to withdraw their money in a pig butchering scheme. SA Krso interviewed 4 of the 6 victims who were defrauded through the same investment site and were each contacted by the same female ("Subject 1") via Facebook. Out of the four victims, only the funds of one victim ("Victim 3") were traced to the SUBJECT ACCOUNT.

20. On November 14, 2023, SA Krso interviewed Victim 3, who at the time resided in Spartanburg, South Carolina. Victim 3 said that on May 9, 2023, Victim 3 met Subject 1 on Facebook. Subject 1 introduced him to an investment website called curve.bet. Victim 3 was instructed and guided by Subject 1 to create an account on Coinbase (cryptocurrency exchange), and how to transfer money from the Coinbase account to the investment website curve.bet. Through curve.bet, Victim 3 was able to see the deposited of Victim 3's money and the appearance of its exponential growth.

21. Based on the fraudulent misrepresentations of Subject 1, Victim 3 sent Subject 1 BTC including on May 16, 2023, to cryptocurrency wallet **3P3UH1saup6Ym1nFUuU7yRR3iF8N6kFTo4 ("FTo4")**; between June 2, 2023, to June 22, 2023, in six transactions to the cryptocurrency wallet **35VbuaJCU9UL8J5JLAf6iHiAtKz2LkkKXb ("kKXb")**; and on or about June 29, 2023, and July 16, 2023, in two transactions to cryptocurrency wallet address **3QhJ83Ut138mruYC1w8iz5m5K66KvwDnB ("wDnB")**.

22. In or around July 2023, Victim 3 said that his balance with curve.bet had risen to approximately \$580,000 USD. Victim 3 said that in or around July 2023, he attempted to transfer \$380,000 from his investment account with curve.bet to Victim 3's Coinbase account but the transfer was unsuccessful. Victim 3 stated that Victim 3 contacted curve.bet online customer support and was advised to send 20% of the \$380,000 USD from Victim 3's Coinbase account to curve.bet for the funds to be released. Further, Victim 3 stated that Victim 3 contacted Subject 1 and asked why Victim 3 could not receive the funds from curve.bet. Victim 3 stated that Subject 1, assured Victim 3 to follow curve.bet instructions and send 20% or \$78,000 USD to the curve.bet account to release the \$380,000 USD transfer from curve.bet. Victim 3 stated that

Subject 1 offered to lend him \$10,000 USD to pay the fee to curve.bet. Victim 3 stated that Subject 1 encouraged Victim 3 to borrow money from others, take out a credit line, and sell his vehicle to come up with the \$78,000 USD. In my training and experience, it is common for perpetrators to offer lending a small portion of money to a victim to convince them to obtain the rest elsewhere and assuage legitimacy concerns. The money being lent from the perpetrator to the victim is fictitious and the perpetrators will notify the victim that they have lent the money and deposited directly to their investment account, which is being controlled by the perpetrators.

23. SA Krso reviewed the nine (9) transactions totaling 3.099175898 BTC sent by Victim 3 utilizing forensic tracing tools and determined that the Victim 3's funds were sent to three different private addresses which were later sent to wallet **xyWE** in the SUBJECT ACCOUNT.

24. SA Krso reviewed the transactional details of the SUBJECT ACCOUNT, which showed that at the time of his review the SUBJECT ACCOUNT wallet had received a lifetime total deposit of approximately 1094.54 BTC, with the majority of the BTC being sent from private wallets. The OKX account records reflect that the U.S. Dollar value of the BTC that had entered the account was approximately \$39,921,266.87 USD.

25. SA Krso conducted a transactional review of OKX records and found that the SUBJECT ACCOUNT's activity included regular trade and internal purchase orders for alternate forms of cryptocurrency, most commonly converting virtual currency from BTC to USDT. Funds were also transferred out of the account. After identifying that the account was likely used to support a scam, law enforcement requested OKX freeze the SUBJECT ACCOUNT pending further investigations.

26. According to OKX, on November 10, 2023, OKX questioned the accountholder about the suspicious activity in the account and asked the accountholder to provide the source of funds in his account. According to OKX, accountholder never provided the source of funds in his

account. According to OKX, on November 11, 2023, accountholder requested that OKX unfreeze his BTC so he could conduct short-term trading.

27. On most occasions, after SUBJECT ACCOUNT received the BTC from the victim, the SUBJECT ACCOUNT holder executed trades on OKX converting the BTC to USDT. Often those funds were then transferred out of the account.

C. Trace Analysis

a. Victim 1 trace analysis of funds to SUBJECT ACCOUNT.

i. Transfer #1 (Victim 1)

28. On August 13, 2022, at 11:08:02 GMT-6, Victim 1 transferred 0.46105146 BTC from hot wallet **bc1q7cyrfmck2ffu2ud3rn5l5a8yv6f0chkp0zpemf** (“pemf”) in Victim 1’s Crypto.com account to wallet **3KaY641aVbut2fSwSsduCZwnXJwBhVZydC** (“ZydC”) (transaction hash: 0797d2819c37e9677d2e1dc1e77786e5e71907d6926c4beae410d63d1035eeb7).

29. Crypto.com is a cryptocurrency exchange company initially founded in Hong Kong, currently based out of Singapore. A hot wallet is a virtual currency wallet that is accessible online, which facilitates cryptocurrency transactions between the owner and end-users. A transaction hash is a unique string of characters that individually identifies every transaction that is verified and added to the blockchain.

30. On August 14, 2022, at 1:12:48 GMT-6, 1.91000000 BTC was transferred from wallet **ZydC** to wallet **E6oy** (transaction hash: 866c26d7e9ead68db56548340365b149da06082946e55df53066cd85db944b8f).

31. On August 14, 2022, at approximately 1:58:36 GMT-6, 3.58000000 BTC was transferred from wallet **E6oy** to wallet **xyWE** in the SUBJECT ACCOUNT (transaction hash: edcf091c01155181ef96e4d6df3d0c35350884edf182774fab1dc546756e2da2).

ii. Transfer #2 (Victim 1)

32. On August 16, 2022, at approximately 9:28:31 GMT-6, Victim 1 transferred 0.14382424 BTC from Victim 1's Crypto.com account. 0.14382424 BTC was transferred from Crypto.com hot wallet **pemf** to wallet **ZydC** (transaction hash: 07bdf5b90cf7de4465fc49da84e82e5771382bca56b6a866ff9d63a38e943094).

33. On August 17, 2022, at approximately 3:26:52 GMT-6, 0.56000000 BTC was transferred from wallet **ZydC** to wallet **E6oy** (transaction hash: ffd11d413f58538e8bd339eb14121463261981482822951e3186603c3459a935).

34. On August 17, 2022, at approximately 4:12:02 GMT-6, 0.96000000 BTC was transferred from wallet **E6oy** to wallet **xyWE** in the SUBJECT ACCOUNT (transaction hash: b2ae920207424a2dca5a140c3c35ecc32f5539600657626ba0117046f56c8916).

iii. Transfer #3 (Victim 1)

35. On August 28, 2022, at approximately 10:52:59 GMT-6, Victim 1 transferred 0.19925890 BTC from Victim 1's Crypto.com account. 0.19925890 BTC was transferred from Crypto.com hot wallet **pemf** to wallet **ZydC** (transaction hash: 3d460bef66c97d98eb57d7235c9867473222d0418e30e36390948af5319f8717).

36. On August 29, 2022, at approximately 01:17:00 GMT-6, 0.61000000 BTC was transferred from wallet **ZydC** to wallet **E6oy** (transaction hash: 799b24b97d2e0107d36b2ba7457728858b89dae0bece503f6ea767a6e081da63).

37. On September 8, 2022, at approximately 07:22:19 GMT-6, 3.00000000 BTC was transferred from wallet E6oy to wallet **xyWE** in the SUBJECT ACCOUNT (transaction hash: 40bd0e291ddbd2739df174310e3172588cbc17e560e367a4353ef787aa030715).

iv. Transfer #4 (Victim 1)

38. On August 30, 2022, at approximately 07:01:18 GMT-6, Victim 1 transferred 0.22242213 BTC from Victim 1's Crypto.com account. 0.22242213 BTC was transferred from Crypto.com hot wallet **pemf** to wallet **ZydC** (transaction hash: eb9e4f2fd05124cd2f8c0d2ca8ec7f488634f6e7a89848549764b27e6e63c5cd).

39. On August 31, 2022, at approximately 1:19:27 GMT-6, 1.92000000 BTC was transferred from wallet **ZydC** to wallet **E6oy** (transaction hash: 1102fdd8c56761580d63ef2da3512ec6daa61b5d8cc3bb9325369872722e0e2e).

40. On August 31, 2022, at approximately 01:49:27 GMT-6, 3.50000000 BTC was transferred from wallet **E6oy** to wallet **xyWE** in the SUBJECT ACCOUNT (transaction hash: bb19cdabe84c77ebffa51a875eaa1e68d4d5565c0b64d0d40002d54b7a53d1b7).

v. Transfer #5 (Victim 1)

41. On September 12, 2022, at approximately 11:18:45 GMT-6, Victim 1 transferred 0.23007720 BTC from Victim 1's Crypto.com account. 0.23007720 BTC was transferred from Crypto.com hot wallet **pemf** to wallet **388pCfua8ruCE4RbdRuCz5ku6nkA4xKpou** ("**Kpou**") (transaction hash: bef1f0705cdb3891af244faa276a01e02ade0234b114a1e8b14ff6a404e58287).

42. On September 13, 2022, at approximately 03:18:21 GMT-6, 0.30063850 BTC was transferred from wallet **Kpou** to wallet **E6oy** (transaction hash: 2bb1dbe79ed71c47d062f96af804625bcaa7751ad60ff77a57b13e0ab73e5932).

43. On 9/13/22 at approximately 04:16:10 GMT-6, 0.30000000 BTC was transferred from wallet **E6oy** to wallet **xyWE** in the SUBJECT ACCOUNT (transaction hash: e2e5a929a58f1e8e750c58a80c5a9ef7c81459d0638045d3a2cfe775a30035e9).

vi. Transfer #6 (Victim 1)

44. On September 13, 2022, at approximately 10:47:57 GMT-6, Victim 1 transferred 0.37996088 BTC from Victim's Crypto.com account. 0.37996088 BTC was transferred from Crypto.com hot wallet **pemf** to wallet **Kpou** (transaction hash: 42a658f51d2049fe20e2ff3bd24446257f54fbcdd6ee84a6a63fc399cae19a0).

45. On September 13, 2022, at approximately 11:10:37 GMT-6, 0.37993478 BTC was transferred from wallet **Kpou** to wallet **ZydC** (transaction hash: 05325f5ef975b5dd3f84559e7ef8b8a8dbfc701153d08dfeaa255d383876161e).

46. On September 14, 2022, at approximately 01:37:56 GMT-6, 1.52000000 BTC was transferred from wallet **ZydC** to wallet **E6oy** (transaction hash: 669d87b629d2014888161096040cf11e342fd22e5b31d8de48ff607a9dd598d2).

47. On September 14, 2022, at approximately 02:02:23 GMT-6, 5.43000000 BTC was transferred from wallet **E6oy** to wallet **xyWE** in the SUBJECT ACCOUNT (transaction hash: e3d535bf43f63752091aad086e22db5417f48dc8c1104509357ea2855c437682).

b. Victim 2 trace analysis of funds to SUBJECT ACCOUNT.

i. Transfer #1 (Victim 2)

48. On June 15, 2023, Victim 2 transferred 0.00765388 BTC from Cash App to suspect wallet address **3PXH23mUQwqkc8nJGdpZ2q4oLXaPWdVJvg** ("**VJvg**") (transaction hash: d833088c1c605d4671ba92fec5e61c00ff97084b69592f1793f4808ecb935bd5).

49. On June 16, 2023, 0.138336 BTC was transferred from wallet **VJvg** to wallet **E6oy** (transaction hash:

b1575190357b70c6cba872d075fae0a3ca67a760e27740952be9aa7165fa37f1).

50. On June 16, 2023, 0.36000000 BTC was transferred from wallet **E6oy** to wallet **xyWE** in the SUBJECT ACCOUNT (transaction hash:

dfa6ecfb2ded8ac6c6915c5f4ffc2fac50767b420497f9058ddd32652a70ec38).

ii. Transfer #2 (Victim 2)

51. On June 16, 2023, Victim 2 transferred 0.03738671 BTC from Cash App to suspect wallet address **VJvg** (transaction hash:

958461e200929aa7ead0d8b985ffb782f17cc38b416da29350691fb47970748e).

52. On June 20, 2023, 0.620908 BTC was sent from wallet address **VJvg** to wallet **E6oy** in the SUBJECT ACCOUNT (transaction hash:

ff9df4641ea8df9f483b5f70cb0053380f38c3431c85b552c191f34e324a6e34).

53. On June 20, 2023, 1.27 BTC was sent from wallet **E6oy** to wallet **xyWE** (transaction hash: 2ee7c324d966c350f9dd7d425b4e26e355470a91b9b5e8e4eec819c412ebf5ba).

iii. Transfer #3 (Victim 2)

54. On June 17, 2023, Victim 2 transferred 0.07428184 BTC from Cash App, to suspect wallet **VJvg** (transaction hash:

47daffec3bfc24de47a6ef9f84b9f3c76e7f48ca1865496aa1e283b161ae4afa).

55. On June 20, 2023, 0.620908 BTC was sent from wallet **VJvg** to wallet **E6oy** (transaction hash: ff9df4641ea8df9f483b5f70cb0053380f38c3431c85b552c191f34e324a6e34).

56. On June 20, 2023, 1.27 BTC was sent from wallet **E6oy** to OKX exchange wallet **xyWE** (transaction hash:

2ee7c324d966c350f9dd7d425b4e26e355470a91b9b5e8e4eec819c412ebf5ba).

iv. Transfer #4 (Victim 2)

57. On July 5, 2023, Victim 2 transferred 0.3224163 BTC from Crypto.com account to suspect wallet **3Q5qsnI82gYSCnVern1yMfKoq81kaZ7Qqq** ("**7Qqq**") (transaction hash: a5b164e02a886ff054593d90000aa985f6ca008671f137102fe8a8c91c505d15).

58. On July 6, 2023, 0.970983 BTC was sent from wallet **7Qqq** to wallet **E6oy** (transaction hash: 0d5ab076a064ec44f66bea1a2c15c8fe8a44eec0a9177fa3a212062e6a3784c2).

59. On July 6, 2023, 4.34 BTC was sent from wallet address **E6oy** to wallet **xyWE** (transaction hash: eacd5873937d2b90de1db013563442f9acb877a5bd83108460ee14000c576840).

c. Victim 3 trace analysis of funds to SUBJECT ACCOUNT

60. On December 6, 2023, SA Krso provided me with a trace analysis, utilizing a TRM Labs tracing tool, of Victim 3's funds that Victim 3 transferred to Subject 1 in nine transactions:

| Transaction Number: | Date: | BTC: | Transaction Hash: |
|---------------------|----------------------|-------------|--|
| 1 | 5/16/2023 0430hrs | -0.14207976 | 07de74376909b36680514110b35c4793030ecd3c1276675807c2b75b102bf25a |
| 2 | 6/3/2023 2412hrs | -0.16007513 | d0ab2bbe5e099fb490c155e4bebe2fd6e1560e16134f95c75beb7650349181e0 |
| 3 | 6/9/2023 2406hrs | -0.21812877 | 3395662512ad6d758d8dc6d3b9a7d445c47d89c211127aeb6aef40ce069e949a |
| 4 | 6/15/2023 0310hrs | -0.10290106 | ca393b7f4c98df6e604cd4261bb284e943c26812295ade3b1018a7534fb081ec |
| 5 | 6/16/2023 1628hrs | -0.3774397 | b336622129474a23ffd57a96ac144f2662d64b44e671679f7b51493dc540ffff |
| 6 | 6/21/2023 2313hrs | -0.74794681 | 3f8239435922d513e606ece3dada347ec12144789d8ba6a3e60516df930d357c |
| 7 | 6/22/2023 1822hrs | -0.7648023 | 4a0d0c3cb8a540796936256f9ee155a433d6dba1e0a767537d7c8d0901225563 |
| 8 | 6/29/2023 1447hrs | -0.52679725 | 05194fff305a002cb6d663e5994d660cf0271d89b7da93285aa8f05ad50700b3 |

| | | | |
|---|----------------------|-------------|--|
| 9 | 7/17/2023 0234hrs | -0.05960608 | 277c67cc8d301a0e4afb27abc8614748b55f3320879f63014ff876523f3aadf7 |
|---|----------------------|-------------|--|

61. In six of the transactions (transactions 2 to 7), wallet **kKXb** was used as the initial deposit wallet.

62. In eight of the transactions (transactions 1 to 8), Victim 3's funds moved through wallet **3JzBC15Q3HQveDuDmUVBzu1AuFhEacCeHG** ("CeHG").

63. The trace analysis showed that Victim 3's funds were ultimately moved to **xyWE** in the SUBJECT ACCOUNT.

i. Transaction #1 (Victim 3)

64. On May 16, 2023, 0430hrs, Victim 3 sent 0.141980008 BTC to Subject 1 wallet **FTo4** (transaction hash:

07de74376909b36680514110b35c4793030ecd3c1276675807c2b75b102bf25a). The next outbound transaction occurred on May 29, 2023, at 2204hrs, when 0.84121908 BTC, which included Victim 3's funds, was sent to wallet address

33C9WDEZQKnFEoQhog7pdnsYtpPrUMdsHE ("dsHE") (transaction hash:

07de74376909b36680514110b35c4793030ecd3c1276675807c2b75b102bf25a). The next outbound transaction occurred on June 16, 2023, at 1334hrs, when 4.42033275 BTC, which included Victim 3's funds, was sent to wallet **CeHG** (transaction hash:

55009743069f87583609ce106da14b2209ce64802057627dca7bb265182589fe). The next outbound transaction occurred on July 3, 2023, at 0739hrs, when 8.09989635 BTC, which included Victim 3's funds from eight of the transactions, was sent to wallet

35BFAF6XuUHz95DGExMjhgqioLMwpJHgYB ("HgYB") (transaction hash:

62bea24a78d391a6680869d57691e1d67a8e7d88ccc4713796cb3ffce35b88a5). On July 3, 2023, at 0831hrs, 8.099 BTC, which included Victim 3's funds from transactions one through eight,

was sent to **xyWE** (transaction hash:

116612386c46e08ca8a318643b2cc5fa31bf6368763ae51ccd4635c3d8b60bac).

ii. Transactions #2 through #7 (Victim 3)

65. After the initial deposit of funds for transactions two through seven as depicted in the table above, Victim 3's funds for each of these transactions were transferred together as follows:

a. On June 22, 2023, at 1846hrs, 1 BTC, which contained Victim 3's funds from transactions two through seven, was transferred to **CeHG** (transaction hash: bd9bbefb055f83d51755bb3ed18236675dc87bad3cf115e645409ec86af2b51f).

b. On July 3, 2023, at 0739hrs, 8.09989635 BTC, which included Victim 3's funds from transactions one through eight, was sent to wallet **HgYB** (transaction hash: 62bea24a78d391a6680869d57691e1d67a8e7d88ccc4713796cb3ffce35b88a5). On July 3, 2023, at 0831hrs, 8.099 BTC, which included Victim 3's funds from transactions one through eight, was sent to **xyWE** (transaction hash: 116612386c46e08ca8a318643b2cc5fa31bf6368763ae51ccd4635c3d8b60bac).

iii. Transaction #8 (Victim 3)

66. On June 29, 2023, at 1447hrs, Victim 3 sent 0.52674657 BTC to Subject 1's wallet **wDnB** (transaction hash: 05194fff305a002cb6d663e5994d660cf0271d89b7da93285aa8f05ad50700b3). On June 29, 2023, at 1503hrs, 1 BTC, which included Victim 3's funds from transaction eight, was sent to consolidated address **CeHG** (transaction hash: 574df98687b8649629aefc6f022bfae8113bb0ed57428d423107c521e3563732). From this point,

Victim 3's funds involved in transaction eight were transferred to **HgYB** and **xyWE** along with Victim 3's funds from transactions two through seven.

iv. Transaction #9 (Victim 3)

67. On July 17, 2023, at 0234hrs, Victim 3 sent 0.05958509 BTC to Subject 1's wallet **wDnB** (transaction hash: 277c67cc8d301a0e4afb27abc8614748b55f3320879f63014ff876523f3aadf7). The next outbound transaction occurred on July 18, 2023, at 1809hrs, when 0.94873565 BTC, was sent to wallet address **3NNsanLd1vQ2CJ2Jg8P2Nb3CS4FQYQrHzC** (transaction hash: 2c129fe574a435d04bed0ec920cd7243de7de3ed1387164c1cea70a1f256620c). The next outbound transaction occurred on July 20, 2023, at 1318hrs, when 6.449 BTC was sent to a non-hosted wallet address at **3JMjHDTJjKPnrvS7DycPAgYcA6HrHRk8UG** ("**k8UG**") (transaction hash: cfd428f5f3edea6a44c1aec97774a1f99c963b8739e620927bec3fb4e6514f60). The tracing analysis showed that wallet **k8UG** received \$564,900 in six transactions from **dsHE**, which was a wallet involved in moving Victim 3's funds in transaction one. Furthermore, **k8UG** received \$81,400 in three transactions from wallet **CeHG**, which was involved in the movement of Victim 3's funds in transactions one through eight.

68. In summary, each of the victims were defrauded by a pig butchering scheme that led them to transfer bitcoin to the perpetrators of the fraud. Tracing analysis determined that funds traceable to all three of the victims ended up in the SUBJECT ACCOUNT after being transferred through various intermediate wallets. Wallet **E6oy** was as used as an intermediate wallet through which both Victim 1 and Victim 2's funds passed through before transfer to the SUBJECT ACCOUNT. Consequently, there is probable cause to believe that the SUBJECT ACCOUNT is being used to store the proceeds of pig butchering fraud. Furthermore, there is

probable cause to believe that any cryptocurrency in the SUBJECT ACCOUNT is connected to such fraud.

OUT OF DISTRICT SEIZURE REQUEST

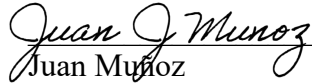
69. Although Rule 41(b) of the Federal Rules of Criminal Procedure provides that search warrants must be executed in the issuing district, other statutes authorize a magistrate to issue a warrant to seize property for forfeiture without regard to its location. For warrants authorizing seizure of property for criminal forfeiture, 21 U.S.C. § 853(l) gives district courts authority to issue criminal seizure warrants under 21 U.S.C. 853(f) “without regard to the location of any property which may be subject to forfeiture.” For warrants authorizing seizure of property for civil forfeiture, 18 U.S.C. § 981(b)(3) gives a judicial officer in any district with jurisdiction over the forfeiture under 28 U.S.C. § 1355(b) to issue a civil seizure warrant that “may be executed in any district in which the property is found, or transmitted to the central authority of any foreign state for service in accordance with any treaty or other international agreement.” Under 28 U.S.C. § 1355(b), this court has jurisdiction over this forfeiture action because “acts or omissions giving rise to the forfeiture” occurred in this district. Consequently, although the SUBJECT ACCOUNT is in the custody of OKX, which is located in Mahe, Seychelles, the court has the authority to issue the requested warrant, which authorizes seizure of that property under both criminal and civil authorities.

CONCLUSION

70. Based on the foregoing, I submit that the above facts establish probable cause to believe that all cryptocurrency in the SUBJECT ACCOUNT is subject to seizure and forfeiture under the authorities listed above. Consequently, I request that the Court issue the proposed seizure warrant. Because the warrant will be served on OKX, who will then collect the funds at a

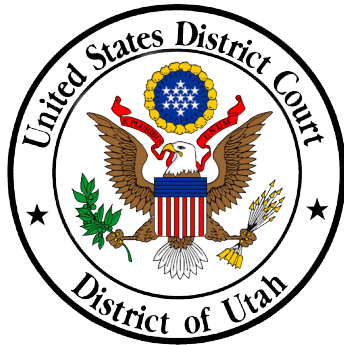
time convenient to it and transfer it to the government, there exists reasonable cause to permit the execution of the requested warrant at any time of the day or night.

I declare under penalty of perjury that the above is true and correct to the best of my knowledge and belief.



Juan Muñoz
Special Agent
Homeland Security Investigations

Attested to by the applicant in
accordance with the requirements
of Fed. R. Crim. P. 4.1 by
telephone on December 11th, 2023





DUSTIN B. PEAB
CHIEF UNITED STATES MAGISTRATE JUDGE